Notice of Allowability	Application No.	Applicant(s)	
	09/918,615	ROGAWAY, PHILLIP W.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *11/28/05*.

2. ☒ The allowed claim(s) is/are *67-70*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

E. Moise

EMMANUEL MOISE
SUPERVISORY PATENT EXAMINER

Allowable Subject Matter

The following is a statement of reasons for the indication of allowable subject matter: Claims 67-68 present an authenticated-encryption method which distinguishes over the prior art. Though the idea of an authenticated-encryption method is known in the prior art and has been done by inventors such as Gligor, the examiner finds no mention of the following claim limitation used in an authenticated-encryption method:

"using the block cipher, the key, and the nonce to generate a sequence of m offsets, each offset having n bits, wherein the sequence of offsets is computed by (a) computing a 0^{th} basis offset by applying the block cipher, keyed by the key, to a constant; (b) for each positive number i, defining the ith basis offset from the prior basis offset by shifting the prior basis offset left one position, and then xoring the resulting value with a constant that depends on the first bit of the prior basis offset; (d) computing a base offset by applying the block cipher, keyed by the key, to the xor of the 0^{th} basis offset and the nonce; (e) defining the 1^{st} offset in the sequence of offsets as the xor of the 0^{th} basis offset and the base offset; and (f) for each integer i between two and m, defining the ith offset in the sequence of offsets as the xor of the prior offset and the jth basis offset, where j is the number of zero-bits following the last one-bit when the number is written in binary".

Furthermore, the examiner does not believe the specific claim limitation above would have been obvious to one of ordinary skill in the art at the time the invention was filed as the limitation is integrally used in the system to form a cohesive approach to performing an efficient authenticated-encryption method.

Claims 69-70 and are also deemed allowable over the prior art. In the previous action, Examiner rejected the claims under Gligor in view of Jutla in further view of Menezes. Upon further consideration, Examiner withdraws the rejection for two reasons: (1) applicant has shown commercial success and (2) the combination fails to meet all the limitations of the claimed invention.

Regarding (1), the applicant has filed a 1.132 declaration which substantially to a declaration that the product has proven commercial success by three separate contracts. Examiner believes that an argument that Gligor in view of Jutla in view of Menezes is weakened by the commercial success.

Regarding (2), examiner does not feel that Menezes, as applied to meet parts (h) and (j) of the claimed invention, teaches length-encoding or xoring of a portion of a block cipher output with a string having length possibly less than the length of the block cipher.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KS

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER